## Patent claims

Sub B1 C1

1. A method for exchanging at least one secret initial value between a processing station and a chip card, in an initializing step for the chip card, wherein
   - first values for determining the secret initial value are generated in the processing station,
   - parts of the first values are transmitted to the chip card,
   - second values for determining the secret initial value are generated in the chip card,
   - parts of the second values are transmitted to the processing station,
   - the secret initial value is determined in the processing station from at least parts of the first values and the transmitted parts of the second values, and
   - the secret initial value is determined in the chip card from at least parts of the second values and the transmitted parts of the first values.
2. A method according to claim 1, characterized in that at least one part of the second values generated in the chip card is generated in accordance with an individual identifier present in the chip card, in particular a serial number.

A

3. A method according to claim 1 ~~or 2~~, characterized in that
   - the first values generated in the processing station are subjected to a first function,
   - the result of the first function is transmitted to the chip card in addition to the part of the first values generated,
   - at least one part of the second values generated in the chip card is subjected to a second function with the transmitted part of the first values,
   - the result of the second function is transmitted to the processing station,
   - the secret initial value is generated in the processing station by means of a third function from the transmitted result of the second function and a part of the first values, in particular the first part of the values not transmitted to the chip card, and
   - the secret initial value is generated in the chip card by means of a fourth function from the transmitted result of the first function, the transmitted

part of the first values and at least one part of the second values, in particular the part of the second values not transmitted to the processing station.

4. A method according to claim 3, characterized in that the first, second, third and fourth functions are identical.

5. A method according to claim 4, characterized in that the function involves exponentiating a first variable with a second variable and forming a modulo residue to a third variable, the variables corresponding to the first and second values and the first and second results.

A

6. A method according to ~~any of claims 1 to 5~~ Claim 1, characterized in that the secret initial value is a start value for generating random numbers.

A

7. A method according to ~~any of claims 1 to 5,~~ Claim 1 characterized in that the secret initial value is a key for encrypting and decrypting data.

8. A method according to claim 7, characterized in that the key generated in processing station and chip card is used in a personalizing step for encrypting and decrypting personalizing data, in particular further secret keys, which are transmitted from the processing station to the chip card.

9. A method according to claim 8, characterized in that the key generated in the processing station and the chip card is deleted in the processing station and the chip card after the personalizing step.